**UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF ILLINOIS**
**EASTERN DIVISION**

| | |
|---|---|
| TREVOR SLOAN, JOSEPH BLEIBERG, ARYEH LOUIS ROTHBERGER, KEVIN FARR, ELMER ORPILLA, and SAGAR DESAI, on behalf of themselves and all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>ANKER INNOVATIONS LIMITED, FANTASIA TRADING LLC, and POWER MOBILE LIFE LLC,<br><br>Defendants. | Case No.: 1:22-cv-07174<br><br>Honorable Sara L. Ellis |

**PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS' MOTION FOR JUDGMENT ON THE PLEADINGS**

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Page(s)**

**Cases**

**Statutes**



**Rules**

## I. INTRODUCTION

Defendants Anker Innovations Limited, Fantasia Trading LLC, and Power Mobile Life LLC's (collectively "Defendants") Motion for Judgment on the Pleadings is an attempt at a second bite at the apple. The Court, in response to the Motion to Dismiss, has already addressed Defendants' extraterritorial arguments, holding that the Illinois Biometric Information Privacy Act ("BIPA") applies to the Illinois Plaintiffs because "the [Eufy Branded Home Security Cameras[1]] provide home security; therefore, the bulk of the circumstances at issue for each individual Plaintiff would occur in his own home." *Sloan v. Anker Innovations Ltd.*, 711 F. Supp. 3d 946, 959 (N.D. Ill. 2024) ("To avoid the extraterritoriality doctrine, 'the circumstances that relate to the disputed transaction [must have] occur[red] primarily and substantially in Illinois,' with 'each case ... decided on its own facts.'") (*citing Avery v. State Farm Mut. Auto. Ins. Co*., 835 N.E.2d 801, 853–54 (Ill. 2005)).[2] Despite this clear ruling, Defendants re-raise the issue under the guise of a Motion for Judgment on the Pleadings.

In order to justify the Court's reexamination of its prior decision, Defendants assert that three new cases—*Campana v. Nuance Commc'ns, Inc*., No. 21 CV 1241, 2024 WL 2809838 (N.D. Ill. Mar. 8, 2024), *McGoveran v. Amazon Web Servs., Inc*., No. 1:20-CV-01399-SB, 2024 WL 4626253 (D. Del. Oct. 30, 2024), and *Vance v. Google LLC*, No. 20-CV-04696- BLF, 2024 WL 1141007, at *4 (N.D. Cal. Mar. 15, 2024) ("*Vance I*")—render the Court's previous analysis erroneous. More specifically, Defendants claim that these cases stand for the proposition that BIPA requires that the "collecting and storing [of] the biometric information . . . occurred in Illinois" and that collecting the "raw precursor information—such as a voice recording, photograph, or video—

[1] "Camera Products" collectively refers to eufycam, Video Smart Lock, SoloCam, Floodlight Cam, Video Doorbell, and Solo Indoorcam lines of home security cameras.

[2] The Court dismissed all BIPA claims, except those of Plaintiffs Sloan and Orpilla (the Illinois based Plaintiffs). Thus, only Plaintiffs Sloan and Orpilla's claims are at issue in the present Motion.

from which biometrics are later created" is not sufficient in-state conduct. Motion, p. 1.

Defendants' argument is fatally flawed for multiple reasons. *First*, Defendants' cases do not mark any change in the law. *See* Motion, p. 6 n.3. These cases do not address, much less displace, the well-established case law holding that collecting photographs from devices in Illinois, for the purposes of conducting facial recognition elsewhere, is sufficient to raise a claim under BIPA, so long as there is some allegation of defendants operating in the state. *See, e.g., Vance v. Microsoft Corp*., 525 F. Supp. 3d 1287, 1293 (W.D. Wash. 2021) ("*Vance II*") (allowing BIPA claims for facial scans that occurred on photos that were uploaded in Illinois, given that Microsoft conducts business in the state: "While Microsoft is correct that Plaintiffs do not allege where Microsoft obtained the dataset [citation], that fact alone may not be dispositive."), *Vance v. Int'l Bus. Machines Corp*., No. 20 C 577, 2020 WL 5530134, at *3 (N.D. Ill. Sept. 15, 2020) ("*Vance III*") (noting that questions regarding extraterritorial application of BIPA to photographs collected from Illinois residents is a fact-intensive analysis that cannot be resolved on the pleadings), and *Vance v. Google LLC*, No. 20-CV-04696-BLF, 2024 WL 5011611, at *3–4 (N.D. Cal. Dec. 5, 2024) ("*Vance IV*") (allowing BIPA claims for facial scans on photos that were uploaded in Illinois, by Illinois residents, given that defendant had engineering staff within the state).

*Second*, these cases recognize that "[t]here is no 'bright-line test for determining whether a transaction occurs within this state ... each case must be decided on its own facts.'" *Campana*, 2024 WL 2809838 at *2 (holding that allegations that harm occurred by dealing with parties in Illinois, executing contracts in Illinois, and a disputed contract containing Illinois choice of law clause were sufficient to establish Illinois connections beyond mere residence); *see also Sloan*, *supra*. Defendants' attempts to synthesize a hard rule from these decisions is misplaced.

*Third*, Defendants' Motion ignores the clear nexus of in-state conduct alleged in the

Complaint,[3] including that Defendants (i) illegally obtained, stored, and disclosed biometric information through the Camera Products purchased by Plaintiff Sloan and Plaintiff Orpilla, which were located at their homes in Illinois and thus captured video, photographs, and biometric information in Illinois (¶¶ 11, 17), (ii) sell and market the Camera Products within Illinois (¶ 27), (iii) provided software that Plaintiffs accessed and used within Illinois (¶ 29), and (iv) had contracts with the Plaintiffs (which were entered into in Illinois) that contain an Illinois choice of law clause (¶ 30). Indeed, it strains credulity to assert that the injury to Plaintiffs Sloan and Orpilla occurred anywhere but Illinois. These substantial connections to Illinois distinguish this case from the "new" case law cited by Defendants.

## II. FACTUAL BACKGROUND

Anker markets, distributes, and sells its "eufy" branded security products, including the Camera Products, throughout the United States, including Illinois. ¶ 27. "These Camera Products are specifically marketed for *home security, allowing consumers to view live and recorded video of the areas around their homes* and to automatically receive notifications on their cell phone, tablet, or computer regarding activity detected by the cameras, including thumbnail images when a person is detected in the cameras' field of view or when a person presses the doorbell." ¶ 27 (emphasis added). "The Camera Products also have the BionicMind system, marketed as a 'local artificial intelligence used for facial recognition.'" ¶ 28. "The BionicMind system enables eufy cameras to differentiate between known individuals and strangers by recognizing biometric identifiers (*i.e.*, details about the face's geometry as determined by facial points and contours) and comparing the resulting 'face template' (or 'faceprint') against the face templates stored in a database." ¶ 28. Either as doorbells or stand-alone security cameras, the Camera Products are often physically affixed to,

[3] References to the "Complaint" are to Plaintiffs' Consolidated Class Action Complaint. ECF No. 31. Citations to "¶ __" or "¶¶ __" are to paragraphs of the Complaint.

or are within, countless houses in Illinois. Accordingly, the Camera Products are intricately linked to Plaintiffs Sloan and Orpilla's Illinois homes and capture information from their residences.

To receive notifications or view their camera feeds, consumers must use the eufy Security smartphone application (the "eufy Security App"). ¶ 29. "The End User License Agreement ("EULA") for the eufy Security App and the Camera Products provides that "you agree that this EULA, and any claim, dispute, action, cause of action, issue, or request for relief relating to this EULA, **will be governed by the laws of Illinois**, without giving effect to any conflicts of laws principles that require the application of the laws of a different jurisdiction." ¶ 30 (emphasis added).

Facial recognition presents substantial consumer privacy concerns since, among other things, an individual's face can be used to open an app, program or cellular phone, and, unlike a password, a face template *cannot* be changed. ¶ 40. Knowing that privacy and security were essential to consumers, Plaintiffs allege that Anker designed and conducted a long-term marketing campaign touting the supposed privacy and security features of the Camera Products. ¶ 31.

For example, each Camera Product label stated that "we're taking every step imaginable to ensure that your data remains private, with you," "your recorded footage will be kept private," data is "transmitted to you, and only you." ¶ 32. The label further warranted that "[a]ll your footage is securely stored locally[,] [e]nsuring the videos you record are for you and only you." *Id.* Defendants' website also included a "privacy policy" that did not disclose that Camera Products collected or stored facial recognition information. ¶ 34. In addition, in the Google and Apple App stores, Defendants represented that "[n]o data [is] shared with third parties." ¶ 36.

These representations, however, were false. On November 23, 2022, security researcher Paul Moore posted a string of tweets demonstrating that the Camera Products were uploading name-tagged thumbnail images, *i.e.* biometric information, to Anker's Amazon Web Services ("AWS") hosted cloud storage without encryption. ¶¶ 42–43. More specifically, Plaintiffs alleged that:

> On November 23, 2022, Moore uploaded a video that demonstrated his findings. With his eufy Homebase unplugged, Moore walked in front of his camera. From an incognito web browser, Moore could pull up a thumbnail image of himself, an image of the feed shortly before he was visible, and—perhaps more concerning—ID numbers indicating his recognized face and his status as the camera owner.[fn] In other words, the Camera Products paired consumers' facial scans with other personally identifiable information from the consumer, which made Defendants capable of determining consumers' identities. This further suggests that all this information had been uploaded to a web server.

¶ 43. Plaintiffs further alleged that "the Camera Products were uploading name-tagged thumbnail images to *Anker's AWS-hosted cloud_storage*." ¶ 42 (emphasis added). Put differently, Defendants were collecting data from Camera Products, when they should have had no access to such data.

Thus, Plaintiffs allege a violation of BIPA:

> Prior to collecting and using Plaintiffs' biometric identifiers, Anker required that each user provide their email address through the eufy Security App. This information enables Defendants to associate the collected biometric identifiers with Plaintiffs' identities, as evidenced in part by the unique ID numbers and name-tagged thumbnail images uploaded to Anker's AWS-hosted cloud storage...

¶ 124. While Defendants attempt to make it seem as if AWS was "an out-of-state third-party vendor," completely unrelated to Defendants' activities, this is not true. Motion, p. 2. AWS offers cloud-based computers for others to rent. In this case, Plaintiffs alleged that Defendants rented their AWS servers to store the biometric data that they collected from Plaintiffs' home security cameras. However, it was the hardware and software on these cameras that created biometric data.

## III. STANDARD ON MOTION FOR JUDGMENT ON THE PLEADINGS

Rule 12(c) permits a party to move for judgment after the complaint and answer have been filed by the parties. *See* Fed. R. Civ. P. 12(c). Courts review Rule 12(c) motions by employing the same standard that the Court applies when reviewing a motion to dismiss under Rule 12(b)(6). *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629, 633 (7th Cir. 2007). Thus, the Court "accept[s] all well-pleaded facts as true and draw[s] all reasonable inferences in the plaintiff's favor." *White v. United Airlines, Inc.*, 987 F.3d 616, 620 (7th Cir. 2021). "Like Rule 12(b) motions, courts grant a

Rule 12(c) motion only if 'it appears beyond doubt that the plaintiff cannot prove any facts that would support his claim for relief.'" *N. Indiana Gun & Outdoor Shows, Inc. v. City of S. Bend*, 163 F.3d 449, 452 (7th Cir. 1998) (citation omitted).

## IV. ARGUMENT

### A. Defendants' Request for Judicial Notice Should not be Granted

As a threshold matter, Defendants request that the Court take judicial notice of AWS's website (Global Infrastructure, Regions and Availability Zones, https://aws.amazon.com/about-aws/global-infrastructure/regions_az/). Motion, p. 4. First, it is difficult for Plaintiffs to assess this request as Defendants did not provide a copy of the website, as it appeared on the date accessed, with its Motion. *Felty v. Driver Sols., LLC*, No. 13 C 2818, 2013 WL 5835712, at *3 (N.D. Ill. Oct. 30, 2013) ("Due to the evolving nature of websites, this Court is neither required nor inclined to take judicial notice of any website material at this time."). Nonetheless, judicial notice "merits the traditional caution it is given, and courts should strictly adhere to the criteria established by the Federal Rules of Evidence before taking judicial notice of pertinent facts." *Gen. Elec. Capital Corp., v. Lease Resolution Corp*., 128 F.3d 1074, 1081 (7th Cir. 1997). Accordingly, courts do not take notice of the truth of matters asserted on websites, due to the "varying levels of reliability" of information found on the internet. *Mussat v. Power Liens, LLC*, No. 13-CV-7853, 2014 WL 3610991, at *3 (N.D. Ill. July 21, 2014) ("this Court declines to take judicial notice of Power Liens' website in order to show the existence of a business relationship."). Here, AWS's website, "without more, is not sufficiently reliable for this Court to take judicial notice of its contents" as evidence of the location of its servers. *Id.*

However, even if the Court was to take judicial notice of this website, it does not support Defendants' claim that no AWS infrastructure is located within Illinois. Motion p. 4. To the contrary, the website specifically provides that AWS maintains edge locations in Chicago. *See*

AWS, *Global Infrastructure, Regions and Availability Zones*, https://aws.amazon.com/about-aws/globalinfrastructure/regions_az/ (last visited March 24, 2025). In addition, the website does not address the fundamental factual questions at issue, including when, where, and how biometric information is uploaded to AWS, and the extent of Defendants' control over these servers. The location of AWS only raises a question of fact that is not, on its own, determinative of the dispute.

**B. Plaintiffs' BIPA Claims Are Adequately Plead**

As Defendants concede, the trio of "recent" cases they cited—*Campana*, *McGoveran*, and *Vance I*—do not represent any new interpretation of the underlying law. *See* Motion at p. 6 n.3. Instead, the geographic reach of BIPA is a case-specific exercise that looks at the underlying relationship between the alleged illegal data collection and Illinois. *Vance II*, 525 F. Supp. 3d at 1292. "There is no single formula or bright-line test for determining whether a transaction occurs within [Illinois]." *Id*. Thus, such "a fact intensive inquiry [is] best left for summary judgment." *Campana,* 2024 WL 2809838 at *2 (*citing Mahmood v. Berbix, Inc*., No. 22 C 2456, 2022 WL 3684636 at *2 (N.D. Ill. Aug. 25, 2022)).

Here, to establish where a BIPA violation occurred, the Court can look to a number of factors, including "plaintiff's residency, the location of harm, where communications between parties occurred, and where a company is carrying out the aggrieved policy." *See Vance II, supra.* In addition, where the "information was accessed" is also relevant. *Id.* Importantly, where biometric information is stored is *not* necessarily relevant to the Court's analysis. This is because BIPA "doesn't penalize mere possession of biometric information." *See King v. PeopleNet Corp.,* No. 21 CV 2774, 2021 WL 5006692, at *8 (N.D. Ill. Oct. 28, 2021). Nor is it dispositive where biometric information is processed (for reasons stated below). Instead, the relevant section of BIPA prohibits the "collection" and "capture" of biometric identifiers or biometric information within Illinois. 740 ILSC 14/15(b) ("No private entity may collect, capture, purchase, receive through

trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information"); *see also, Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 965–66 (N.D. Ill. 2020) ("*Heard I*") ("Unlike Sections 15(a), (c), (d), and (e) of the BIPA—all of which apply to entities 'in possession of' biometric data—Section 15(b) applies to entities that 'collect, capture, purchase, receive through trade, or otherwise obtain' biometric data. Recognizing this distinction, the parties agree that mere possession of biometric data is insufficient to trigger Section 15(b)'s requirements." (citations omitted)). Defendants' myopic focus on where biometric information was *processed or stored* is irrelevant to the underlying claim. Instead, the relevant question is where Defendants illegally "collect," "capture" or "otherwise obtain" access to Plaintiffs' biometric information. *Id.*

Defendants strain logic and the law by claiming that they did not "collect" any biometric information within Illinois because "AWS servers were [not] in Illinois or that Defendants otherwise accessed their biometrics in Illinois in any other way." Motion, p. 7-8. As noted above, Plaintiffs allege that Defendants represented that the "Camera Products also have the BionicMind system, marketed as a 'local artificial intelligence used for facial recognition.'" ¶ 28. Plaintiffs further allege that Defendants represented that all data from the Camera Products is "transmitted to you, and only you" and that "[a]ll your footage is securely stored locally[,] [e]nsuring the videos you record are for you and only you." ¶ 32. Accordingly, whether the biometric data is taken from Defendants' AWS server or the Camera Products themselves, the result is the same: Defendants illegally "collect[ed]," "captur[ed]" or "otherwise obtain[ed]" biometric data in violation of BIPA in Illinois. 740 ILSC 14/15(b). This is because such data *should have never left* Plaintiff Sloan's and Plaintiff Orpilla's Illinois-based Camera Products in the first place.[4] That Defendants obtained

[4] Plaintiffs concede that there are some questions regarding how exactly the BionicMind

biometric information (or that it was transmitted to Defendants' servers) is evidence enough that it was illegally obtained. *Figueroa v. Kronos Inc*., 454 F. Supp. 3d 772, 783–84 (N.D. Ill. 2020) (allegations that the defendant stored data sufficed for § 15(b) liability because in order to store data, the defendant "necessarily first had to 'obtain' the data").

In addition, the collection of biometric information occurred in this state. While Defendants assert that "Plaintiffs' presence in Illinois is not sufficient for the Court to make a reasonable inference that Defendants' alleged conduct occurred primarily and substantially in Illinois," this is not what was alleged. Motion, at pp. 8-9. Defendants correctly note that the Court already held that Defendants allegedly accessed Plaintiffs' data without their consent, and this data collection occurred "at their residence, where they had installed the cameras." Motion, p. 8 n.4, ECF No. 66 at 12–13. And there is no reason to displace this finding. The Complaint alleged that Plaintiffs Sloan and Orpilla are Illinois citizens who reside in Illinois. ¶¶ 11, 17. The "collection" of biometric information occurred from Camera Products located in their Illinois homes. *Id.*

Further, any injury to Plaintiffs Sloan and Orpilla's privacy (*i.e.* the purported illegal collection of biometric information without their consent from their home security cameras), occurred within Illinois. This is sufficient to allege a violation of BIPA. *Vance II*, 525 F.Supp.3d 1293 (allowing BIPA claims for facial scans of photos that were taken in Illinois, uploaded in Illinois by Illinois residents, and performed by defendant that conducts business in Illinois); *Vance III*, 2020 WL 5530134, at *1–3 (allegations that plaintiff uploaded photographs to the photo sharing service Flickr from a computer in Illinois, which were than used for facial recognition software by a third party, were sufficient to allow the case to continue to discovery). Finally,

system works. Nevertheless, such factual questions are not a reason to dismiss a case at the pleading phase. *Vance II*, 525 F.Supp.3d at 1292 ("the majority of courts in BIPA cases to consider the issue at this stage have denied the motion to dismiss, opting instead to allow discovery for more information regarding the extent to which the alleged misconduct occurred in Illinois.").

Defendants specifically market and directly sell their Camera Products and eufy Security App within Illinois. ¶¶ 19-22. Defendants' conduct within the State is sufficient to satisfy BIPA.

Defendants waste much ink on where the facial recognition data was actually created. *See* Motion, p. 8 ("the biometrics themselves never existed in this state, but were created only elsewhere (on the out-of-state AWS servers)") & n.4 ("in Plaintiffs' own words, facial recognition was not happening 'at their residence.'"). This is irrelevant for two reasons: *First*, the Complaint specifically alleges that "Anker collected and captured facial recognition information from Plaintiffs and Class members, as well as their friends and family that appear on their cameras" and "[t]his information was then uploaded to Anker's servers, and stored there, without notice, prior consent, or providing a publicly available policy establishing a retention schedule and guidelines for permanently destroying this Biometric Data." ¶ 53. The Court has already held that these allegations are sufficient to allege a BIPA violation. *Sloan v*, 711 F. Supp. 3d at 958 ("Considering the allegations that the eufy products used the BionicMind programs to construct faceprints and Defendants stored facial recognition data on the cloud together, Plaintiffs have described a scheme that 'plausibly constitutes scans of face geometry.'"). At this stage of the litigation, the Court must accept these allegations as true. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

*Second*, BIPA does not turn on whether facial recognition data has first been conducted/processed before the corresponding data was transmitted to Defendants. Instead, the statute prohibits the collection, capture, purchase, receipt through trade, or otherwise obtaining both "customer's biometric identifier or biometric information" without consent. Under BIPA, "biometric information" is defined as "*any information*, *regardless of how it is captured*, converted, stored, or shared, *based on an individual's biometric identifier used to identify an individual*." 740 ILCS 14/10 (emphasis added). And "biometric identifiers" includes face geometry scans. *Id.* Thus, "[w]hile photographs alone do not support a BIPA action, photographs

used by a system that can take a geometric scan of a person do qualify as biometric data." *Sloan,* 711 F. Supp. 3d at 958 (*citing Sosa v. Onfido, Inc*., 600 F. Supp. 3d 859, 871 (N.D. Ill. 2022) ("But nothing in section 10 expressly excludes information derived from photographs from the definition of biometric identifiers."). Even if Defendants only scanned a person's face from a photo that they collected from the Illinois-based Camera Products, the result would be the same as if Defendants collected the facial scan from the electronic storage on the Camera Products themselves. *See, e.g., Rivera v. Google Inc*., 238 F. Supp. 3d 1088, 1091, 1095–97 (N.D. Ill. 2017) (Plaintiffs who were the subject of photographs taken by smartphones, and whose photographic images were automatically uploaded, without their consent, to a cloud-based service that scanned facial features to create face templates, sufficiently alleged a violation of BIPA); *In re Facebook Biometric Info. Priv. Litig*., 185 F. Supp. 3d 1155, 1171 (N.D. Cal. 2016) (Users' allegations that social networking website scanned their uploaded photographs and used their faces as biometric identifiers, without their consent, in tool that automatically matched names to faces on pictures uploaded to the site, were sufficient to state a claim under BIPA); *ACLU v. Clearview AI, Inc.*, No. 20 CH 4353, 2021 WL 4164452, at *1, *5 (Ill. Cir. Ct. Aug. 27, 2021) (creating a faceprint by scanning publicly-available internet photos, measuring and recording data such as the shape of the cheekbones and the distance between eyes, nose, and ears constituted a scan of face geometry in violation of BIPA).

Indeed, when determining the extraterritorial effect of a statute, the Illinois Supreme Court cautions that it makes "little sense" to focus on one out-of-state element of a transaction, when the "bulk of the circumstances that make up a [ ] transaction occur within Illinois." *Avery*, 835 N.E.2d at 853. Here, the vast majority of the relevant facts, including "plaintiff's residency," "the location of harm," "where communications between parties occurred," and "information was accessed" all point squarely at Illinois. *Vance II*, 525 F. Supp. 3d at 1292. The fact that some data may have been processed or stored out-of-state is not dispositive. *Patel v. Facebook, Inc*., 932 F.3d 1264,

1276 (9th Cir. 2019) ("[I]t is reasonable to infer that the General Assembly contemplated BIPA's application to individuals who are located in Illinois, even if some relevant activities occur outside the state."). This is particularly true here, where *Defendants elected* to have "any claim, dispute, action, cause of action, issue, or request for relief relating to the EULA [ ] governed by the laws of Illinois." ¶ 26. There is no reason to displace the application of BIPA under such circumstances. *LaSalle Bank Nat'l Assoc v. Paramont Properties*, 588 F. Supp. 2d 840, 849 (N.D. Ill. 2008) ("Illinois courts honor a contractual choice of law clause provided that (1) it does not contravene a fundamental policy of Illinois, and (2) the state chosen bears a reasonable relationship to the parties or the transaction."); *M. Block & Sons, Inc. v. IBM Corp*., No. 04 C 340, 2004 WL 1557631, at *4 (N.D. Ill. July 8, 2004) ("The clause states that the laws of New York will govern any 'rights, duties and obligations arising from, or relating in any manner to, the subject matter of this Agreement.' This provision indicates that the parties intended New York law to apply broadly to matters related to or arising out of the contractual obligations.").

**C. Defendants' Case Law Does Not Support Their Request**

Defendants' citations to *Campana*, *McGoveran,* and *Vance I* do not call for entry of judgment here. While Defendants state that these three cases stand for the proposition that "a plaintiff's residence in Illinois [is not] enough to show that a BIPA violation occurred 'primarily and substantially in Illinois,'" Plaintiffs do not stand on mere residency. Motion, pp. 5-6. Again, Plaintiffs Sloan and Orpilla are Illinois residents, who alleged that photographs and facial recognition data were taken from their Illinois-based Camera Products, without permission. These products were specifically marketed by Defendants within the State, and Plaintiffs Sloan and Orpilla purchased the Camera Products in Illinois. And Plaintiffs Sloan and Orpilla bolster their argument by noting the EULA specifically provided the present claims would be governed by the laws of Illinois. Plaintiffs Sloan and Orpilla alleged a substantial nexus between their BIPA claims

and the state of Illinois beyond mere Illinois residency.

To illustrate, in *Campana*, plaintiff alleged that she called the FedEx customer service hotline to inquire about a package and interacted with a "Voice ID" authentication system, in violation of BIPA. *Campana,* 2024 WL 2809838 at *1. The *Campana* plaintiff did not allege any other connections to Illinois other than her residency at the time of the call. *Id.*, at *2. Under such circumstances, *Campana* found that such facts were not sufficient to invoke Illinois law. *Id.* But, the *Campana* Court specifically differentiated the facts before it with a case where a "plaintiff alleged that she scanned her fingerprints in Illinois using the defendant's hardware and the hardware stored her fingerprints in Illinois." *Id.*, at *3 (*citing Ronquillo v. Doctor's Assocs., LLC*, 597 F. Supp. 3d 1227, 1234 (N.D. Ill. 2022)). Moreover, *Campana* also noted cases which held that the presence of an Illinois choice of law clause combined with a transaction that occurred in Illinois was sufficient to allege instate conduct. *Id.,* at *2 (*citing Morrison v. YTB Int'l, Inc*., 649 F.3d 533, 538 (7th Cir. 2011)). The facts of this case are much closer to the facts of the cases distinguished by *Campana* than the facts of *Campana* itself.

Similarly, in *McGoveran,* plaintiff alleged that defendants extracted biometric information from calls originating from Illinois with clearly recognizable Illinois phone numbers. *McGoveran,* 2021 WL 4502089, at *4. However, the defendants (who plaintiffs called) were all out-of-state entities and all of the relevant voice *capture* and *analysis* occurred out-of-state. *Id.* Thus, the *McGoveran* Court found that "Plaintiffs' concrete allegations about this case's connections to Illinois are nothing more than repeated statements (phrased three different ways) about Plaintiffs' residency." *Id.* The *McGoveran* Court had concerns that extending liability in such situations would harm "a vast number of corporations who do no business in Illinois and who lack any other significant connection to Illinois." *Id.,* *6. The same concerns are not at issue here. Again, Defendants' Camera Products took the active step of transmitting data created by the Camera

Products, within the State of Illinois, without permission. Defendants also sold their Products within Illinois and understood that their actions could subject them to Illinois law, because that is what the EULA provided. This is a far cry from imposing liability under BIPA because an Illinois-based consumer called an out-of-state business which had no connections to Illinois.

The facts of *Vance I* are even more far removed from this case. In *Vance I*, plaintiffs alleged that they uploaded their photographs to a website hosted by Flickr from their Illinois-based devices. *Vance I,* 2024 WL 1141007 at *1. Flickr then compiled millions of Flickr photographs, including plaintiffs' photographs, into the "Flickr Dataset" and made the dataset publicly available. *Id.* IBM then used images culled from the Flickr Dataset to create the Diversity in Faces Dataset ("DiF Dataset") for improving the ability of facial recognition systems to fairly and accurately identify individuals across diverse populations. *Id.* This data included "biometric identifiers of Plaintiffs taken from the Flickr Dataset, by scanning the facial geometry of facial images." *Id.* Defendant Google obtained the DiF Dataset to improve its own facial recognition technology. *Id*. the *Vance I* plaintiffs did not allege that "Google ever interacted with them or any other person or entity in Illinois to obtain the DiF Dataset." *Id.,* at *3.

*Vance I* is not analogous to the case at bar. Here, Plaintiffs allege that the Illinois based Camera Products were programmed, by Defendants, to send biometric information to Defendants, that these Camera Products were accessed in Plaintiffs' Illinois homes, and Defendants sold and marketed the Camera Products in Illinois. ¶¶ 19, 25, 42. While Defendants try to force this case into the *Vance I* mold, their efforts are futile. The involvement of AWS in this case is not remotely similar to the intervening actions of Flickr and IBM in *Vance I.* Plaintiffs allege that "the Camera Products were uploading name-tagged thumbnail images to Anker's AWS-hosted cloud storage" and Defendants "collected biometric identifiers with Plaintiffs' identities, as evidenced in part by the unique ID numbers and name-tagged thumbnail images uploaded to Anker's AWS-hosted

cloud storage." ¶¶ 42, 124; *see also* ¶ 55 ("Defendants eventually admitted that they were already aware that their eufy cameras transmitted images and biometric information to their AWS-hosted cloud storage."). Accordingly, Plaintiffs specifically alleged that it was Defendants that hosted and stored the biometric information on their AWS servers. There are no allegations that AWS did anything but provide cloud storage for Defendants. Nonetheless, the nature of AWS's relationship with Defendants is not something that should be decided at this stage of the case. *See Heard v. Becton, Dickinson & Co*., 524 F. Supp. 3d 831, 841 (N.D. Ill. 2021) ("*Heard II*") (Plaintiff sufficiently that the defendant's device scans the user's fingerprint and then stores users' biometric information both on the device and in defendant's servers and questions regarding what entities' servers actually stored store users' biometric information were to be resolved later in the case).

It is also worth noting that the Northern District of California ultimately allowed the allegations in *Vance I* to move forward. In *Vance IV*, the court found that plaintiffs alleged sufficient connections with Illinois by stating that Google used the DiF Dataset on products partially engineered in Illinois and that the "DiF Dataset obtained by Defendant included photographs of Plaintiffs, who were Illinois residents, and significant information about those photographs." *See Vance IV, supra,* at *3. This brings the Northern District of California in line with courts in this District which found BIPA applied under similar facts. *See, e.g., Vance III*, 2020 WL 5530134, at *1–3 (allegations that plaintiff uploaded photographs to the photo sharing service Flickr, from a computer in Illinois, which were then used for facial recognition software by a third party, were sufficient to allow the case to continue to discovery). *Vance I* does not control, has been supplanted by *Vance IV*, and is inapposite.

## V. CONCLUSION

As set forth above, the Court should deny Defendants' Motion in its entirety.

Dated: April 4, 2025

Respectfully submitted,

**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC**

/s/ *Trenton R. Kashima*
Trenton R. Kashima
402 West Broadway, Suite 1760
San Diego, CA 92101
Telephone: (619) 810-7047
tkashima@milberg.com

Gary M. Klinger
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: 866.252.0878
gklinger@milberg.com

Nick Suciu III
6905 Telegraph Rd., Suite 115
Bloomfield Hills, MI 48301
Telephone: (313) 303-3472
nsuciu@milberg.com

**POMERANTZ LLP**

Brian Calandra
Jeremy A. Lieberman
600 Third Avenue, 20th Floor
New York, New York 10016
Telephone: (212) 661-1100
Facsimile: (212) 661-8665
bcalandra@pomlaw.com
jalieberman@pomlaw.com

**LEVI & KORSINSKY, LLP**

Mark S. Reich
Gary I. Ishimoto
55 Broadway, 10th Floor
New York, NY 10006
Telephone: 212-363-7500
Facsimile: 212-363-7171
mreich@zlk.com
gishimoto@zlk.com

**KOZYAK TROPIN &**
**THROCKMORTON LLP**

Robert J. Neary
Abe Bailey
2525 Ponce de Leon Blvd., 9th Floor
Coral Gables, FL 33134
Telephone: (305) 372-1800
Facsimile: (305) 372-3508
rn@kttlaw.com
abailey@kttlaw.com

**RENNERT VOGEL**
**MANDLER & RODRIGUEZ, P.A.**

Robert M. Stein
Daniel S. Maland
100 SE 2nd Street, 29th Floor
Miami, FL 33131
Telephone: (305) 423-3437
Facsimile: (305) 376-6176
rstein@rvmrlaw.com
dmaland@rvmrlaw.com

*Counsel for Plaintiffs and the Putative Classes*

**CERTIFICATE OF SERVICE**

I hereby certify that on this 4th day of April, 2025, I caused a true and correct copy of the foregoing notice to be filed with the Clerk of the Court for the Northern District of Illinois via the Court's CM/ECF system, which will send notification of such filing to the counsel of record in the above-captioned matters.

*/s/ Trenton R. Kashima*
Trent R. Kashima